UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
v.	)	CASE NO. 04CR10217GAO
DARREN F. WILDER	)	

DEFENDANT'S MOTION IN LIMINE TO PRECUDE EVIDENCE AND TESTIMONY REGARING ENCASE FORENSIC SOFTWARE AND INCORPORATED MEMORANDUM OF LAW

NOW COMES the Defendant, Darren Wilder, through counsel, and respectfully moves this Honorable Court purusant to Fed.R.Evid., Rules 702, 703 and 704, to preclude the Government from offering any evidence or expert testimony at trial regarding data retrieved from the Defendant's computers using the EnCase forensic software. In support thereof, counsel states the following.

INTRODUCTION

On January 15, 2004, the Government seized tow computers from the Defendant's residence pursuant to a search warrant. The Government's forensic analysis of the computer included the use of the EnCase forensic software to retrieve deleted files and images on the computers. In fact, all of the evidence relating to Counts 1 & 3, and the last six images set forth in Count 2, of the Second Superceding Indictment were obtained using EnCase.[1] By the instant

[1] It is the Defendant's position that the remaining images which allegedly were not deleted, do not contain "sexually explicit conduct". *See* Defendant's Motion in Limine to Preclude the Government from Introducing Evidence of Images Allegedly Obtained from the Defendant's Computer Which do not Depict Minors Engaged in "Sexually Explicit Conduct" as

motion in limine the Defendant seeks to exclude evidence and the testimony of the Government's prospective expert witnesses because the EnCase program fails to meet the requirment of Rules 702, 703 and 704. Like DNA testing, forensic computer analysis must meet the same strict standards for admissiblity. It is not sufficient that EnCase may be the best computer forensic recovery tool available to law enforcement.

ARGUMENT

I. THE METHODOLOGY ON WHICH THE EXPERT'S TESTIMONY IS BASED DOES NOT SATISFY THE *DAUBERT* ANALYSIS AND MUST BE EXCLUDED.

The Government seeks to offer evidence and expert testimony regarding deleted files allegedly recovered by the Government from the Defendant's computers using a computer forensic software tool known as EnCase. See Summary of the National Institute of Standards and Technology (NIST) Report entitled "*Test Results for Disk Imaging Tools: EnCase 3.20*, June 2003 ("Summary"), a copy of which is attached hereto as Exhibit "1".[2] This Report is a result of the Computer Forensics Tool Testing ("CFTT") project, representing the joint effort of the National Institute of Justice, ("NIJ"), the National Institute of Standards and Technology ("NIST"), the U.S. Department of Defense, the Technical Support Working Group, and other related agencies to "provide measurable assurance ... that the tools used in computer forensics

---

Defined in 18 U.S.C. Section 2256 and Incorporated Memorandum of Law.

[2]A copy of this document can be obtained from the Department of Justice's website, at http://www.ojp.usdoj.gov/nij/pubs-sum/200031.htm.

investigations provide accurate results." See "Introduction" to the Report, p. 4.[3]

As the proponent of this evidence, the Government bears the burden of showing that the "expert's conclusion has been arrived at in a scientifically sound and methodologically reliable fashion," in accordance with Daubert standards. See United States v. Mahone, 328 F.Supp.2d 77, 87 (D.Me. 2004), citing United States v. Mooney, 315 F.3d 54, 63 (1st Cir. 2002) (quotation omitted).

The Supreme Court in Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), identified four factors which a court should consider in determining whether to admit the substance of a proffered expert's testimony: (1) whether the theory or technique can be or has been tested; (2) whether the technique has been subject to peer review and publication; (3) the technique's known or potential error rate; and (4) the level of the theory or technique's acceptance within the relevant discipline. Daubert, supra, 509 U.S. at 593-94.

The technique on which the Government expert's proffered testimony rests is a computer forensic software tool known as EnCase, which "allows investigators to examine hard drives and disks for deleted, hidden, and/or renamed computer files." See Summary, Exhibit A. In June, 2003, the NIST issued the aforementioned report, *Test Results for Disk Imaging Tools: EnCase 3.20*, detailing the NIST's test results for disk imaging tools, *i.e.*, EnCase 3.20. The Report describes three anomalies found during the testing of EnCase 3.20 against the disk imaging

[3]Copies of the pages relevant to this discussion and cited herein are attached hereto as Exhibit "C". A copy of the complete NIST report can be obtained from the Department of Justice's website at www.ncjrs.gov/pdffiles1/nij/200031.pdf.

requirements in *Disk Imaging Tool Specification, Version 3.1.6*. Specifically, the following anomalies were found: (1) BIOS anomaly; (2) logical restore anomaly; and (3) restore size anomaly. The NIST stated:

> The behavior observed in these anomalies should not be interpreted as *necessarily* representing unacceptable behavior for an imaging tool. Some of the anomalies may only need more detailed documentation by the tool vendor. However, the tool user must be aware of these behaviors since they *may affect the quality and completeness* of a forensic investigation.

See NIST Report, Exhibit C, p. 6, §2 (emphasis added).

More significantly, the NIST Report states that the deleted file recovery tool of the EnCase software was not subject to testing:

> Test cases that met the following criteria were designated as not applying to EnCase testing:
>
> * Some test cases are going to be deleted from the test specification and are not *ever* used to test any disk imaging tools. For example, *cases involving deleted file recovery are being deleted from the specification because deleted file recovery tools will be tested separately*.

See NIST Report, Exhibit A, p. 11, §3.1 (emphasis added).

Thus, the methodology on which the Government's expert will testify - the deleted file recovery tool of EnCase software - was not, by the Government's own admission, within the category of those computer forensic investigatory tools tested by the Government for accuracy. Nor, to the best of defense counsel's knowledge, has the deleted file recovery tool of EnCase software been tested by any other agency. Without such testing, the deleted file recovery tool of the EnCase software cannot have a known or potential rate of error. The absence of testing also renders the other two factors cited in Daubert - the technique's acceptance within the relevant discipline and peer review and publication of the technique - without value in establishing the

software's reliability.

And, while Guidance Software, Inc., the creator of EnCase software, cites three cases in which EnCase software successfully survived a Frye or Daubert hearing, see Guidance Software Legal Journal, Nov. 2005, citing State v. Nhouthakith, (2001), at pp. 68-69 & n. 144 (Nebraska); State v. Leavell, (2000), at pp. 64-65 & n. 134 (Washington); and People v. Rodriguez, (2001), at pp. 65-66 (California),[4] none of those decisions were published, and each case occurred prior to the NIST's Report stating that no testing of the deleted file recovery tool took place.

Defendant acknowledges that a trial judge has broad latitude to employ other factors when evaluating reliability. Mooney, supra, 315 F.3d at 62, citing Kumho Tire, 526 U.S. at 153. Yet given the lack of testing of the deleted file recovery aspect of the EnCase software and the absence of its known or potential error rate, this part of the EnCase software cannot be declared reliable within the parameters of Daubert. As the First Circuit has observed: "[M]ethodology remains the central focus of a Daubert inquiry." See Mahone, supra, 328 F.Supp.2d at 90, citing Ruiz-Troche v. Pepsi Cola of P.R. Bottling Co., 161 F.3d 77, 81 (1st Cir. 1998).

Accordingly, consistent with Fed.R.Evid. 702's gatekeeping function of keeping those expert opinions which are not the product of reliable principles and methods from reaching the trier of fact, the testimony of the Government's witnesses pertaining to deleted files allegedly recovered from the Defendant's computers using the EnCase software deleted file recovery tool should be excluded.

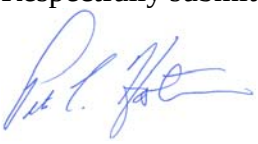
---

[4]This report can be obtained from the Guidance Software website at http://www.guidancesoftware.com/corporate/downloads/whitepapers/Legal JournalNovember 2005.pdf.

CONCLUSION

WHEREFORE, based on the foregoing points and authorities, this Honorable Court is respectfully urged to exclude the proposed evidence and expert testimony.

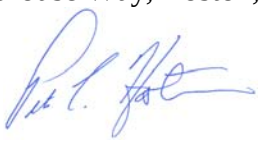
Respectfully submitted,



Peter Charles Horstmann, Esquire
BBO #556377
PARTRIDGE, ANKNER & HORSTMANN, LLP
200 Berkeley Street, 16th Floor
Boston, Massachusetts 02116
(617) 859-9999

CERTIFICATE OF SERVICE

I, Peter Charles Horstmann, Esquire, hereby certify that on this 20th day of February, 2006, a copy of the foregoing motion was served electronically upon Sherri Stephan, Trial Attorney, U.S. Department of Justice Child Exploitation and Obscentiy Section, 1400 New York Avenue, NW, 6th Floor, Washington, DC 20005, and Dana Gershengorn, Assistant United States Attorney, United States Attorneys Office, One Courthouse Way, Boston, MA 02210



Peter Charles Horstmann, Esquire